

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 Claim 1 (original): A communications method for use in a system
2 including comprising a first, second and third nodes, and a
3 first secret, said first secret being shared between the first
4 and second nodes to secure communications between said first and
5 second nodes, the method comprising:
6 operating the first node to establish a secure
7 communications session with said second node using the first
8 shared secret to secure the contents of packets communicated
9 from the first node that are directed to the second node as part
10 of the secure communications session;
11 operating a third node which is coupled to said first and
12 second nodes to maintain in memory a copy of said first shared
13 secret; and
14 operating the third node to receive a secure flow of
15 packets from the first node that are directed to said second
16 node as part of the secure communications session.

1 Claim 2 (original): The method of claim 1, further comprising:
2 operating the third node to receive from said second node
3 the first shared secret and to store the first shared secret in
4 memory, said received first shared secret being encrypted using
5 a second shared secret known to the second and third nodes.

1 Claim 3 (original): The method of claim 2, further comprising:
2 operating said third node to receive and process packets
3 sent from said first node as part of said established
4 communications session, said third node sending a message to the
5 first node indicating successful receipt of packets by said
6 second node.

1 Claim 4 (original): The method of claim 3, wherein said third
2 node uses said first shared secret to secure the message to the
3 first node.

1 Claim 5 (original): The method of claim 5, wherein said third
2 node operates as an application proxy for said second node
3 during said secure communications session without informing said
4 first node that the third node is acting as a proxy in the place
5 of said second node.

1 Claim 6 (original): The method of claim 5, further comprising:
2 operating the third node to transmit information obtained
3 from said communications session while said third node was
4 acting as a proxy for said second node to said second node; and
5 operating the second node to continue the secure
6 communications session with the first node.

1 Claim 7 (original): The method of claim 1, further comprising:
2 operating the third node to inspect the secure packet flow
3 from the first node, said step of inspecting said secure packet
4 flow including performing at least one of a group of security
5 steps which use the first shared secret, said group of security
6 steps comprising: decrypting a packet, integrity checking
7 contents of a packet, and authenticating a sender of a packet.

1 Claim 8 (original): The method of claim 7, further comprising:
2 operating the third node to drop the packet from the packet
3 flow if the performed at least one of the group of security
4 checks fails.

1 Claim 9 (original): The method of claim 7, further comprising:
2 operating the third node to additionally process the
3 packets from the packet flow if no performed security check in
4 said group of security checks fails.

1 Claim 10 (original): The method of claim 9, further comprising:
2 operating the third node to identify a packet with a
3 disallowed packet payload by comparing at least a portion of the
4 payload of each packet in the packet flow to information
5 indicating allowed packet payloads, payloads of a type which are
6 not indicated by said information being disallowed packet
7 payloads.

1 Claim 11 (original): The method of claim 10, further
2 comprising:
3 operating the third node to drop an identified packet with
4 a disallowed packet payload.

1 Claim 12 (original): The method of claim 10, further
2 comprising:
3 operating the third node to modify the packet payload of
4 packets identified to include a disallowed packet payload based
5 on stored information indicating payload modifications to be
6 made to disallowed packet payloads.

1 Claim 13 (original): The method of claim 12, wherein the
2 modified payload generated by modifying a packet payload
3 includes a message indicating that an erroneous payload was
4 detected at the third node.

1 Claim 14 (original): The method of claim 10, further
2 comprising:
3 operating the third node to process at least two packets in
4 the packet flow to produce at least a third packet.

1 Claim 15 (original): The method of claim 9, further comprising;
2 operating the third node to generate an additional packet
3 flow from the received packet flow directed to the second node
4 and to forward the additional packet flow to the second node,

5 packets in said additional packet flow having a source address
6 corresponding to the first node and a destination address
7 corresponding to the second node, said step of generating an
8 additional packet flow including at least one of a group of
9 security steps which use the first shared secret, the group of
10 security steps consisting of: encrypting a packet, adding an
11 integrity check for the contents of the packet, and adding an
12 authenticator check for the packet sender.

1 Claim 16 (original): The method of claim 1, wherein the second
2 and third nodes each include a second secret used to secure
3 communications between the third node and the second node, the
4 method further comprising:

5 operating the third node to generate an additional packet
6 flow from the received packet flow directed to the second node
7 and to forward the additional packet flow to the second node,
8 packets in said additional packet flow having a source address
9 corresponding to the third node and a destination address
10 corresponding to the second node, said step of generating an
11 additional packet flow including at least one of a group of
12 security steps which use the second shared secret, the group of
13 security steps consisting of: encrypting a packet, adding an
14 integrity check for the contents of the packet, and adding an
15 authenticator check for the packet sender.

1 Claim 17 (original): The method of claim 16, further
2 comprising:

3 operating the second node to communicate the first shared
4 secret to the third node, the first shared secret being
5 encrypted using the second shared secret.

1 Claim 18 (original): The method of claim 17, further
2 comprising:

3 mutually authenticating the second and third nodes prior to
4 the second node transmitting the first shared secret to the
5 third node.

1 Claim 19 (original): A communications system, comprising:

2 a first node including a first shared secret and a
3 communications application for establishing a secure
4 communications session using said first shared secret to secure
5 packets communicated as part of said secure communications
6 session;

7 a mobile node including said first shared secret, a second
8 shared secret, and at least one communications application for
9 maintaining a secure communications session with said first node
10 using said first shared secret;

11 an intermediate node, coupled to said first node and said
12 mobile node, said intermediate node including said first shared
13 secret and said second shared secret, said intermediate node
14 including:

15 means for processing packets directed by said first
16 node towards said mobile node as part of a secure
17 communications session using said first shared secret; and

18 means for sending a message to said first node secured
19 by said first shared secret indicating successful receipt
20 of said packets by said mobile node.

1 Claim 20 (original): The communication system of claim 19,
2 wherein said intermediate node further includes:

3 means for communicating information generated by processing
4 packets directed to said mobile node to said mobile node in
5 packets secured using said second shared secret, said
6 information being the result of application processing performed
7 on the payload of at least two data packets to generate
8 information not present in either of the two data packets.

1 Claim 21 (original): The communication system of claim 20,
2 wherein the mobile node includes means for sending said first
3 shared secret to said intermediate node in an encrypted format
4 resulting encryption processing using said second shared secret.